CLAIMS

1. (Currently Amended) A processing system comprising:

a central processor~~,~~;

a BIOS memory device storing a boot program;

~~and~~ a BIOS protection device;

a plurality of memory address and data paths to provide communication between at least the processor, BIOS memory device and BIOS protection device; ~~interconnected by address and data paths~~, said BIOS protection device configured to verify the boot program and ~~wherein at start-up, the BIOS protection device takes~~ control ~~of~~ the memory address and data paths and prevent[[s]] execution of [[a]] the boot program ~~stored in the BIOS memory device~~ until said verification. ~~the BIOS protection device has verified that the boot program stored in the BIOS memory device is authentic.~~

2. (Currently Amended) The system as claimed in claim 1 wherein the BIOS protection device is in communication between ~~connected to the processing system between~~ a central processor and the BIOS memory device, the BIOS protection device configured to ~~including~~ include address and data path interface connections, and an authentication processor, ~~whereby, when power is applied to the BIOS protection device,~~ the BIOS protection device configured to ~~takes~~ control ~~of~~ the address and data path(s) to which it is connected and the authentication processor configured to interrogate[[s]] the BIOS memory device connected to the address and data path(s) to determine if the boot program contained in the BIOS memory device is authentic, and ~~only~~ if the boot program is determined to be authentic ~~does the BIOS protection device release control of the address and data path(s) to~~ permit execution of ~~the central processor to execute~~ the boot program.

3. (Currently Amended) The system as claimed in claim 2 wherein the address and data path interfaces are selected from a group comprising ~~comprise one of~~ a serial interface, a totally non- multiplexed bus, an Intel™ Low Pin Count (LPC) bus structure.

4. (Original) The system as claimed in claim 2 wherein the address and data path interfaces comprise an Intel™ Low Pin Count (LPC) bus structure.

5. (Currently Amended) The system as claimed in claim 1, wherein the BIOS memory device includes a cryptographic structure ~~digital signature~~ located at a known location in the BIOS memory device.

6. (Currently Amended) The system as claimed in claim 5 wherein the BIOS protection device cryptrographic structure is a digital signature and the BIOS protection device is configured to calculate[[s]] the value of the cryptographic ~~digital signature~~ structure from contents of the BIOS memory device and an internal public key and interrogates the BIOS memory device to verify that the correct cryptrographic structure ~~signature~~ is present and corresponds with the boot program, or a part thereof stored in the BIOS memory device.

7. (Currently Amended) The system as claimed in claim 1 wherein the BIOS protection device also contains an internal memory device and is configured to, while authenticating the BIOS memory device contents, ~~the BIOS protection device copies~~ copy at least part of the BIOS memory device contents to the internal memory device and ~~subsequently~~ control[[s]] the address and data path(s) to bypass the BIOS memory device and communicate[[s]] with the internal memory device ~~instead~~ when the central processor attempts to access the copied part of the BIOS memory device contents.

8. (Currently Amended) The system as claimed in claim 1 wherein the central processor, the BIOS memory device and the BIOS protection device are mounted on a motherboard configured to be ~~on which at least one signal line of the motherboard is interrupted by the BIOS protection device such that the motherboard is~~ inoperative if the BIOS protection device is not present.

9. (Original) The system as claimed in claim 8 wherein a reset control circuit is provided in the BIOS protection device such that the mother board cannot exit the reset state if the BIOS protection device is not present.

10. (Original) The system as claimed in claim 9 wherein the BIOS protection device will hold the reset signal in the reset (or, disabled) state while the authentication of the BIOS is performed.

11. (Original) The system as claimed in claim 10 wherein when the authentication is successful, the BIOS protection device releases the reset signal allowing the central processor to commence operation.

12. (Original) The system as claimed in claim 1 wherein the BIOS protection device inserts wait cycles to disable the central processor while authenticating the BIOS memory device.

13. (Currently Amended) A method of authenticating a boot program held in a BIOS memory device of a processing system comprising a central processor, the BIOS memory device and a BIOS protection device interconnected by address and data paths, the method comprising :

1) at start-up, the BIOS protection device temporarily prevents execution of the boot program by the central processor;

2) the BIOS protection device takes control of the address and data paths;

3) the BIOS protection device interrogates the contents of the BIOS memory device to establish if the contents are authenticated;

4) if the contents of the BIOS memory device are not authentic, the BIOS protection device continues to prevent execution of the boot program and prevents further operation of the central processor; and

5) if the contents of the BIOS memory device are authentic, the BIOS protection device relinquishes control of the address and ~~datapaths~~ data paths and allows the central processor to execute the boot program in the BIOS memory device.

14. (Original) The method as claimed in claim 13 wherein the address and data paths are interfaced via one of a serial interface, a totally non- multiplexed bus, an Intel™ Low Pin Count (LPC) bus structure.

15. (Original) The method as claimed in claim 14 wherein the address and data paths are interfaced via an Intel™ Low Pin Count (LPC) bus structure.

16. (Original) The method as claimed in claim 13, wherein a cryptographic digital signature is provided at a known location in the BIOS memory device.

17. (Original) The method as claimed in claim 16 wherein the value of the cryptographic digital signature is calculated by the BIOS protection device from contents of the BIOS memory device and an internal public key and the BIOS protection device interrogates the BIOS memory device to verify that the correct signature is present and corresponds with the boot program, or a part thereof stored in the BIOS memory device.

18. (Original) The method as claimed in claim 13 wherein the BIOS protection device also contains an internal memory device and while authenticating the BIOS contents, the BIOS protection device copies at least part of the BIOS memory device contents to the internal memory device and subsequently controls the address and data path(s) to bypass the BIOS device and communicate with the internal memory device instead when the central processor attempts to access the copied part of the BIOS memory device contents.

19. (Original) The method as claimed in claim 13 wherein the central processor, the BIOS memory device and the BIOS protection device are mounted on a motherboard on which at least one signal line of the motherboard is interrupted by the BIOS protection device whereby the motherboard is not operative when the BIOS protection device is not present.

20. (Original) The method as claimed in claim 19 wherein a reset control circuit is provided in the BIOS protection device whereby the mother board does not exit the reset state if the BIOS protection device is not present.

21. (Original) The method as claimed in claim 20 wherein, while the authentication of the BIOS is performed, the BIOS protection device holds the reset signal in the reset (or, disabled) state.

22. (Original) The method as claimed in claim 21 wherein, when the authentication is successful, the BIOS protection device releases the reset signal and the central processor commences operation.

23. (Original) The method as claimed in claim 13 wherein the BIOS protection device inserts wait cycles to disable the central processor while authenticating the BIOS memory device.

24. (Original) A BIOS protection device for connection to a processing system between a central processor and a BIOS memory device containing a boot program, the BIOS protection device including address and data path interface connections, and an authentication processor whereby, when power is applied to the BIOS protection device, the BIOS protection device takes control of address and data path(s) to which it is connected and the authentication processor interrogates the BIOS memory device connected to the address and data path(s) to determine if the boot program contained in the BIOS memory device is authentic, and only if the boot program is determined to be authentic does the BIOS protection device release control of the address and data path(s) to permit the central processor to execute the boot program.

25. (Original) The device as claimed in claim 24 wherein the address and data path interfaces comprise one of a serial interface, a totally non- multiplexed bus, an Intel ™ Low Pin Count (LPC) bus structure.

26. (Original) The device as claimed in claim 25 wherein the address and data path interfaces comprise an Intel™ Low Pin Count (LPC) bus structure.

27. (Original) The device as claimed in claim 24, wherein the BIOS memory device includes a cryptographic digital signature located at a known location in the BIOS memory device.

28. (Original) The device as claimed in claims 27 wherein the BIOS protection device calculates the value of the cryptographic digital signature from contents of the BIOS memory device and an internal public key and interrogates the BIOS memory device to verify that the correct signature is present and corresponds with the boot program, or a part thereof stored in the BIOS memory device.

29. (Original) The device as claimed in claim 24 wherein the BIOS protection device also contains an internal memory device and while authenticating the BIOS contents, the BIOS protection device copies at least part of the BIOS memory device contents to the internal memory device and subsequently controls the address and data path(s) to bypass the BIOS device and communicate with the internal memory device instead when the central processor attempts to access the copied part of the BIOS memory device contents.

30. (Original) The device as claimed in claim wherein the central processor, the BIOS memory device and the BIOS protection device are mounted on a motherboard on which at least one signal line of the motherboard is interrupted by the BIOS protection device such that the motherboard is inoperative if the BIOS protection device is not present.

31. (Original) The device as claimed in claim 30 wherein a reset control circuit is provided in the BIOS protection device such that the mother board cannot exit the reset state if the BIOS protection device is not present.

32. (Original) The device as claimed in 31 wherein the BIOS protection device will hold the reset signal in the reset (or, disabled) state while the authentication of the BIOS is performed.

33. (Original) The device as claimed in claim 32 wherein when the authentication is successful, the BIOS protection device releases the reset signal allowing the central processor to commence operation.

34. (Original) The device as claimed in claim 24 wherein the BIOS protection device inserts wait cycles to disable the central processor while authenticating the BIOS memory device.

35. (Original) A processing system comprising a processor connected to a BIOS memory device containing a boot program through a connection path, wherein a BIOS protection device forms part of the connection path, the BIOS protection device operable to check the authenticity of the boot program and allow the processor to execute the boot program only if the check of the boot program indicates that it is authentic